SINOPSE DO CASE: Segurança da Informação nas organizações[1]

Gyovanna Bianca Garcês Pinheiro da Costa
Anderson Henrique da Silva dos Santos
Davi Borges Duailibe Costa
Davi Santos Rodrigues
Gabriel Araújo Coelho
Arlison Wady Sousa Martins

1 DESCRIÇÃO DO CASO

No caso apresentado, é retratado ao leitor a respeito do aumento significativo de ataques cibernéticos, sendo esse aumento de 330%, durante a pandemia de Covid-19. Diante desse contexto, nitidamente preocupante, cerca de 83% das organizações empresariais no Brasil, com uma rápida resposta, buscaram aumentar o investimento em segurança cibernética. A necessidade nesse investimento torna-se ainda mais claro quando os resultados da pesquisa *PwC Digital Trust Insights* são levados em consideração, onde a mesma revela aos leitores que o número de empresas que preveem um aumento nos gastos cibernéticos para os anos seguintes é maior entre as companhias e organizações do Brasil.

Além disso, vale ressaltar que o frequente aumento na atividade hacker está diretamente relacionado à implementação do trabalho remoto durante a pandemia, como explicado pelo analista de dados, Claudio Bonel. Com um maior volume de acesso remoto, onde as pessoas acessam dados importantes diretamente de casa, os sistemas se tornam mais vulneráveis à invasão.

Dentro deste contexto, com a ajuda da empresa Berghem - *Smart Information Security*, na atuação da área de LGPD (Lei Geral de Proteção de Dados) têm-se a missão de produzir um mapeamento de dados e realizar uma auditoria de segurança da informação nos setores da organização que contratou os serviços da Berghem, a fim de apontar todas as melhorias necessárias para entregar o relatório de impacto. Tendo em vista que a organização

1 Sinopse de case apresentado à disciplina de Segurança e Auditoria de Sistemas, do Centro Universitário Unidade de Ensino Superior Dom Bosco – UNDB.
2 Graduando (a) do 5º Período do Curso de Engenharia de Software do Centro Universitário Unidade de Ensino Superior Dom Bosco – UNDB.
3 Professor da disciplina de Segurança e Auditoria de Sistemas do 5º Período do curso de Engenharia de Software do Centro Universitário Unidade de Ensino Superior Dom Bosco – UNDB

que contratou os serviços da Berghem é uma *fintech* de empréstimos financeiros 100% on-line, é de suma importância garantir a conformidade com a LGPD, pois lida com uma grande quantidade de dados pessoais sensíveis, como informações financeiras e de crédito dos clientes.

2 IDENTIFICAÇÃO E ANÁLISE

A empresa *fintech* que oferece empréstimos online enfrenta desafios cada vez maiores no que diz respeito à segurança de dados, especialmente diante do aumento considerável de ciberataques durante a pandemia de Covid-19. Torna-se essencial a realização de auditorias de segurança da informação não apenas para cumprir com a LGPD, mas também para resguardar as informações sensíveis dos clientes e manter a reputação da empresa intacta.

2.1 Questões para análise

Principais questões:

- De que forma a auditoria de sistema de informação deve ser realizada nos setores da empresa, a fim de apontar todas as melhorias necessárias para entregar o relatório de impacto?

- Como o roteiro deve ser organizado, a fim de demonstrar como a auditoria deve ocorrer?

Questões norteadoras para auxiliar na solução da questão principal:

- Tendo em vista os pilares de sistema de informação, como eles se aplicam ao cenário apresentado, onde as organizações empresariais no Brasil estão aumentando o investimento em segurança cibernética em resposta ao aumento dos ataques cibernéticos?

- Qual o ciclo de vida de uma auditoria e como esse ciclo de vida se aplica à auditoria de segurança da informação que deve ser realizada na Berghem - *Smart Information Security*?

- Tendo em vista os pontos de contato dos titulares, como esses pontos de contato podem ser afetados pelos ataques cibernéticos e quais medidas podem ser tomadas para protegê-los?

- Como manter integridade, confidencialidade e disponibilidade de dados e de que maneira esses princípios se aplicam ao cenário apresentado, onde a empresa que contratou os serviços é uma *fintech* de empréstimos financeiros 100% on-line e precisa garantir a conformidade com a LGPD?

2.2 Possíveis soluções

2.2.1

2.3 Descrição das decisões possíveis

a) 1ª decisão possível:

Implementação de Medidas de Segurança Técnicas e Organizacionais:

Implementação de medidas técnicas como criptografia de dados, controle de acesso, SIEM e autenticação multifatorial para garantir a segurança de dados e conformidade com os requisitos da LGPD.

b) 2ª decisão possível:

Avaliação de Políticas e Processos:

Realizar uma revisão detalhada das políticas e procedimentos existentes da empresa em relação à proteção de dados. Identificar lacunas e áreas de não conformidade com os requisitos da LGPD**.**

2.4 Argumentos capazes de fundamentar cada decisão

a) 1ª Decisão Possível:

A implementação de medidas técnicas, como criptografia de dados e controle de acesso, é fundamental para proteger os dados confidenciais dos clientes contra acesso não autorizado. Por exemplo, a criptografia garante que os dados sejam protegidos durante a transmissão e armazenamento, evitando que terceiros não autorizados acessem os dados. Da mesma forma, os controles de acesso garantem que apenas indivíduos autorizados possam visualizar ou modificar dados sensíveis, reduzindo significativamente o risco de violação de segurança. Além das medidas técnicas, as medidas organizacionais, como a implementação de formação em segurança, ajuda a educar os funcionários sobre as melhores práticas de segurança e os riscos potenciais associados ao manuseio inadequado de dados. Também, o estabelecimento de políticas e procedimentos de segurança claros fornece diretrizes claras para todos os funcionários, promovendo uma forte cultura de segurança e garantindo a conformidade com políticas internas e regulamentos externos. Inclusive, a implementação de um sistema de gerenciamento de eventos e informações de segurança (SIEM) se destaca como uma solução completa para a supervisão de dados. Visto que, através da coleta de dados, correlação e exploração de logs provenientes de diversas fontes, como servidores, dispositivos de rede e aplicativos, o SIEM viabiliza uma visão integrada da postura de segurança da empresa. Ao identificar padrões de comportamento suspeitos e anomalias nos registros, o SIEM possibilita a detecção proativa de ameaças cibernéticas, como tentativas de acesso não autorizado, ataque de *malware* e violações de dados.

b) 2ª Decisão Possível

Uma revisão completa das políticas e procedimentos existentes é fundamental, pois pode fornecer informações sobre práticas atuais da empresa fintech em relação à proteção de dados. Identificar lacunas e áreas de não conformidade é necessário para evitar possíveis

violações e possíveis penalidades legais. Além disso, esta avaliação oferece a oportunidade de alinhar políticas e procedimentos aos princípios da LGPD, garantindo que a empresa opere conforme as melhores práticas de proteção de dados. Propor ajustes e atualizações em políticas e procedimentos é essencial para garantir o comprimento da LGPD e aprimorar a proteção dos dados dos clientes, pois ao identificar áreas onde as práticas atuais podem ser melhoradas, a *fintech* pode tomar medidas proativas para reduzir risco e garantir uma abordagem robusta à proteção de dados. Esses ajustes também podem ajudar a aumentar a transparência e a confiança do cliente, demonstrando um compromisso claro com a proteção da privacidade e o comprimento das regulamentações aplicáveis**.**

3 Descrição dos critérios e valores

3.1 Para alcançar os resultados mencionados anteriormente, foram essenciais seguir as diretrizes da LGPD e realizar pesquisas extensas. Além disso, a adesão rigorosa às normas de segurança da informação desempenhou um papel fundamental na obtenção dos resultados esperados.

Para proteger contra acesso não autorizado, foram implementadas medidas técnicas, como criptografia de dados sensíveis, políticas de acesso restrito e sistemas de detecção de intrusões. Medidas de segurança física, como controle de acesso e proteção de dispositivos de armazenamento, também foram adotadas. Além disso, a conscientização dos funcionários sobre segurança da informação foi aumentada por meio de treinamentos regulares e diretrizes claras sobre a manipulação e compartilhamento de dados. Essas práticas garantiram a conformidade com a LGPD e protegem a integridade e confidencialidade dos dados, conforme as leis e regulamentos aplicáveis.

REFERÊNCIAS

COSTA, C. A.. A aplicação da Linguagem de Modelagem Unificada (UML) para o suporte ao projeto de sistemas computacionais dentro de um modelo de referência. **Gestão & Produção**, v. 8, n. 1, p. 19–36, abr. 2001.

SOBRENOME, Nome. **Título:** subtítulo. Local: Editora, ano. Nº p.

SOBRENOME, Nome. Título do capítulo. In: SOBRENOME, Nome. **Título:** subtítulo. Local: Editora, ano. p. Nº-Nº

SOBRENOME, Nome. Título do capítulo. In: SOBRENOME, Nome. **Título:** subtítulo. Local: Editora, ano. p. Nº-Nº. Disponível em: <link>. Acesso em: dia mês abreviado ano

SOBRENOME, Nome. Título**:** subtítulo. **Revista**, Local, ano Nº, v. Nº, n. Nº, p. Nº-Nº, data ou intervalo de publicação.

SGNFO. [Artigo] Gerenciamento e Correlação de Eventos de Segurança, conheça o Octopus SIEM. Disponível em: <https://seginfo.com.br/2020/07/09/artigo-gerenciamento-e-correlacao-de-eventos-de-seguranca-conheca-o-octopus-siem/>. Acesso em: 24 abr. 2024.